Penetration Testing Server Sistem Informasi Manajemen dan *Website* Universitas Kristen Petra

Richard Pangalila [1], Agustinus Noertjahyana [2], Justinus Andjarwirawan [3]
Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Kristen Petra
Jln. Siwalankerto 121 – 131 Surabaya 60236
Telp. (031)-2983455, Fax. (031)-8417658
rp@richardpangalila.com [1], agust@petra.ac.id [2], justin@petra.ac.id [3]

ABSTRAK

Sebuah organisasi yang berkembang memerlukan teknologi informasi dalam kegiatan operasionalnya. Namun yang sering menjadi pertimbangan adalah bagaimana cara mengamankan data yang ada di *server* dari pihak yang tidak bersangkutan. Dalam penelitian ini, akan diulas bagaimana seorang yang ditugaskan menjadi penganalisa keamanan untuk melakukan pengujian penetrasi dalam suatu sistem dengan diberikan alat - alat yang beragam dan bagaimana laporan hasil analisa bisa dimengerti oleh banyak pihak baik atasan hingga *programmer*. Selain itu penelitian ini juga menjadi tolak ukur sejauh mana organisasi yang dievaluasi ini sudah bisa mengamankan datanya dari pihak yang seharusnya tidak mendapatkan akses terhadap data yang penting dalam kegiatan operasional.

Kata Kunci: Keamanan, Data, Evaluasi, Pengujian Penetrasi

ABSTRACT

A developing organization need information technology in its operational activity. However what is often considered is how to ensure that data saved in server is safe from unauthorized parties. Therefore, this thesis reviews how a person who is appointed as a security analyst do penetration testing in a system with variety tools given and how the report can be understood from by people from managers to programmers. Besides giving the how-to knowledge, this thesis also reviews how secure is the organization under review in keeping their data safe from other parties who are not supposed to get access to important operational activity data.

Keywords: *Safety, Data, Evaluation, Penetration Testing*

1. LATAR BELAKANG

Suatu organisasi yang menjalankan kegiatan operasional yang berbasis teknologi informasi pasti akan menggunakan komputer. Seiring dengan perkembangan teknologi, diperlukan suatu media penyimpanan maupun pusat data yang banyak disebut sebagai *server*. Namun dengan perkembangan teknologi tersebut, keamanan merupakan aspek yang perlu diwaspadai oleh setiap pihak yang memiliki skema sistem terpusat, karena pembobolan, manipulasi, maupun kehilangan data dapat terjadi jika dilakukan oleh para *hacker* yang memang berniat mengambil data sensitif dari sebuah organisasi.

Untuk dapat mengurangi kerugian yang diakibatkan oleh para *hacker*, maka langkah awal yang harus dikembangkan adalah melakukan evaluasi terhadap keamanan *server* yang ada. Hal ini bertujuan untuk mengurangi resiko terjadinya penyalahgunaan terhadap sumber daya yang ada pada organisasi.

Sebagian besar orang di organisasi akan merasa bingung saat diminta untuk melakukan evaluasi keamanan *server* yang ada. Hal ini dikarenakan memang banyak orang yang merasa awam dengan melakukan evaluasi *server*. Istilah *Penetration testing* atau yang lebih dikenal dengan *Pentesting* adalah salah satu metode yang dapat digunakan untuk melakukan analisa terhadap suatu objek yang ingin dipenetrasi.

Pertumbuhan Universitas Kristen Petra semakin besar dan memiliki berbagai macam sistem informasi dalam menjalankan kegiatan operasionalnya. Universitas Kristen Petra sendiri telah memiliki beberapa *server* yang ada di setiap gedung besar seperti, Gedung P, Gedung Radius Prawiro, dan Gedung T. Dengan adanya ketersediaan jaringan di setiap gedung, baik melalui *Wi-Fi* maupun kabel *Ethernet*, maka perlu diperhatikan keterkaitannya antara jaringan dan *server* dari para *hacker*. Pusat Komputer di Gedung utama Universitas Kristen Petra, Gedung Radius Prawiro, adalah tempat yang memiliki *server* induk yang memegang dasar sistem kegiatan akademik mahasiswa.

Selain itu, *human behavior* dari mahasiswa maupun karyawan ini sendiri juga perlu dilihat mengingat bahwa pelaku *hacking* ini adalah manusia sendiri. Terkadang, *human behavior* yang kurang baik ini dapat membawa dampak buruk baik secara langsung maupun tidak langsung.

Oleh karena adanya permasalahan tersebut maka kebutuhan yang penting saat ini adalah membantu meminimalisir dan mengantisipasi *server* yang ada dari kejahatan *hacking*. Salah satu hal yang dapat dilakukan adalah dengan melakukan *monitor* pada *server* yang berada di Pusat Komputer Gedung Radius Prawiro dan melakukan *penetration testing*.

2. LANDASAN TEORI

2.1 Keamanan Komputer

Tujuan dari keamanan komputer adalah melindungi informasi komputer yang berada di dalamnya. Keamanan komputer sendiri meliputi beberapa aspek seperti yang tercantum di modul *Ethical Hacking and Countermeasures*, antara lain :

Privacy, adalah sesuatu yang bersifat rahasia (*private*) dimana ada pembatasan hak akses oleh orang tertentu saja.

Confidentiality, adalah pemberian data ke pihak lain tetapi tetap dijaga penyebarannya.

Integrity, adalah informasi yang tidak boleh diubah kecuali oleh pemilik informasi.

Authentication, adalah verifikasi pengguna melalui tampilan *login* dengan menggunakan nama *user* dan kata sandinya, jika cocok diterima dan sebaliknya.

Availability, adalah kesediaan data saat dibutuhkan.

Adapun beberapa langkah untuk mengamankan komputer seperti yang terlampir dalam modul *Ethical Hacking and Countermeasures*, yakni:

Aset, Perlindungan aset merupakan hal yg penting dan merupakan langkah awal dari berbagai implementasi keamanan komputer.

Analisa Resiko, identifikasi terhadap resiko yang mungkin terjadi, seperti sebuah *event* yang berpotensial untuk mengakibatkan kerugian terhadap sistem.

Keamanan jaringan, semua perangkat yang tersambung pada jaringan perlu diperhatikan keamanannya.

Tools, *tool* yang digunakan pada PC memiliki peran penting dalam hal keamanan karena tool yang digunakan harus benar – benar aman.

Prioritas, perlindungan PC secara menyeluruh.

2.2 *Certified Ethical Hacking*

Certified Ethical Hacker adalah sertifikasi profesional yang disediakan oleh *International Council of E-Commerce Consultants* (EC-Council).

Hacker beretika biasanya dipekerjakan oleh organisasi yang mempercayakan mereka untuk melakukan uji penetrasi pada jaringan atau sistem komputer dengan metode yang umumnya digunakan oleh para *hacker* untuk mencari dan memperbaiki celah keamanan. Jika *hacking* dilakukan tanpa otorisasi perusahaan, maka hal tersebut termasuk dalam *cyber crime*, tetapi hal sebaliknya jika diminta oleh korban atau perusahaan maka dianggap legal.

Hacker yang bersertifikasi memiliki sertifikasi dalam cara mencari celah keamanan dan kelemahan sistem dan menggunakan pengetahuan serta *tools* yang sama selayaknya seorang *hacker*.

Bersumber pada situs EC-Council, kode ujian sertifikasi ini adalah 312-50 dan sertifikasinya berada di versi ke-8 per tahun 2013. EC-Council menawarkan sertifikasi lainnya yaitu *Certified Network Defense Architect* (CNDA). Sertifikasi ini didesain untuk agen pemerintahan Amerika dan hanya tersedia di beberapa agensi tertentu saja dengan nama yang berbeda namun isinya tetap sama. Kode ujian CNDA adalah 312-99.

2.3 *Penetration Testing*

Berdasarkan definisi dalam modul CEH, *Penetration Testing* merupakan metode evaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya dan merupakan bagian dari *security audit*. Simulasi serangan yang dilakukan dibuat seperti kasus yang bisa dibuat oleh *black hat hacker*, *cracker*, dan sebagainya. Tujuannya adalah menentukan dan mengetahui macam – macam serangan yang mungkin dilakukan pada sistem beserta akibat yang bisa terjadi karena kelemahan sistem.

Dalam melakukan *penetration testing*, diperlukan analisa intensif untuk setiap kerentanan yang diakibatkan oleh kelemahan sistem. Nantinya setelah seluruh analisa selesai dilakukan, akan didokumentasikan dan diberikan kepada pemilik beserta solusi dan dampak yang dapat diakibatkan dari celah keamanan yang ada.

3. METODOLOGI PENETRATION TESTING

3.1 Teknik Penetration Testing

Hal – hal yang perlu diuji dalam *penetration testing* ada banyak, hal ini dibutuhkan untuk mengidentifikasi ancaman – ancaman utama seperti kegagalan komunikasi, *e-commerce*, dan kehilangan informasi rahasia. Selain itu ketika berhadapan dengan infrastruktur publik, seperti situs, *gateway e-mail*, akses jarak jauh, DNS, kata sandi, FTP, IIS, dan *server* situs, pengujian dilakukan pada semua perangkat keras dan lunak di sebuah sistem keamanan jaringan.

Adapun faktor – faktor pendukung seperti tujuan, batasan, dan penyesuaian prosedur yang diperlukan untuk membuat *penetration testing* lebih maksimal. Selain hal tersebut diperlukan orang yang professional untuk melakukannya serta pertimbangan biaya yang sesuai dengan kebutuhan. Pada akhirnya diperlukan juga dokumentasi yang jelas serta penjelasan mengenai potensi resiko dan hasil penemuan dari hasil analisa dan uji coba kepada klien.

Bersumber pada modul *Licensed Penetration Tester*, beberapa teknik yang umum digunakan dalam *penetration testing* adalah sebagai berikut :

1. *Passive Research* : digunakan untuk mencari semua informasi umum yang digunakan sebuah organisasi
2. *Open Source Monitoring* : keterbukaan sebuah perusahaan untuk integritas informasi dan kerahasiaan informasinya
3. *Network Mapping* dan OS *Fingerprinting* : digunakan untuk mendapatkan konfigurasi jaringan yang akan diuji coba
4. *Spoofing* : uji coba penyamaran sistem yang disamarkan seperti sebuah komputer yang sudah terdaftar dalam sistem, serta diuji coba dari sisi internal maupun eksternal
5. *Network sniffing* : penangkapan data yang berjalan dalam sebuah jaringan
6. *Trojan Attacks* : kode jahat yang biasanya dikirim dalam sebuah jaringan berupa *attachment* pesan elektronik atau dikirim melalui pesan instan di sebuah ruang *chat*
7. *Brute-Force Attack* : teknik yang umum untuk membuka kata sandi dan dapat membuat sebuah sistem *overload* maupun berhenti merespon ke semua permintaan akses
8. *Vulnerability Scanning* : pemeriksaan menyeluruh pada sebuah area target dari infrastruktur jaringan perusahaan
9. *Scenario Analysis* : pengujian akhir yang melibatkan pengujian dan penilaian resiko celah keamanan lebih akurat dengan sebuah kasus.

3.2 Ruang Lingkup *Penetration Testing*

Dalam sebuah *penetration testing*, diperlukan batasan – batasan yang diperlukan untuk mencakup kebutuhan analisa secara jelas. Terbagi menjadi dua yakni, uji coba destruktif dan non destruktif. Dalam hal ini uji coba non destruktif berisikan mencari dan mengidentifikasi sistem *remote* untuk potensi celah, kemudian menginvestigasi dan verifikasi penemuan serta memetakan setiap celah dengan eksploit yang tersedia. Selanjutnya sistem dieksploitasi dengan hati – hati untuk menghindari gangguan dan memberikan bukti konsep serangan tersebut mungkin dilakukan atau tidak, akan tetapi pengujian ini tidak akan menyebabkan *Denial of Service*. Sebaliknya, dalam pengujian destruktif setelah semua celah dipetakan maka serangan *Denial of Service* dan *Buffer Overflow* dilakukan.

3.3 Jenis *Penetration Testing*

Seperti yang terlampir dalam modul LPT, ada pengelompokan yang membagi tim *penetration testing* yaitu kelompok biru dan kelompok merah. Hal ini memperlihatkan pengujian dilakukan dari segi mana. Kelompok biru merupakan mereka yang menguji dengan pengetahuan dan persetujuan dari pegawai IT dan biayanya relatif lebih rendah serta kebutuhan peran utama untuk memikirkan bagaimana sebuah serangan dadakan dilakukan. Sebaliknya untuk kelompok merah, mereka melakukan pengujian tanpa

sepengetahuan pegawai IT namun dengan persetujuan dari atasan perusahaan, pengujian boleh dilakukan tanpa maupun dengan peringatan, tujuannya adalah mendeteksi jaringan dan celah sistem serta pemeriksaan keamanan dari sudut pandang pendekatan penyerang kepada infrastruktur.

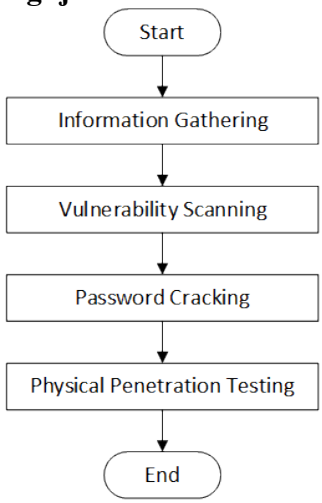
Selain pengelompokan yang disebutkan, ada jenis – jenis *penetration testing* yakni *black-box* atau *penetration testing* eksternal, *white-box* atau *penetration testing* internal baik yang diumumkan maupun tidak. Ada juga beberapa pihak yang menggunakan kedua jenis pengujian.

Metode *black-box* merupakan jenis *penetration testing* yang serupa dengan *hacker* aslinya karena penguji hanya diberikan nama perusahaan saja dan informasi mengenai jaringan maupun informasi lainnya harus dicari sendiri oleh penguji, cara ini merupakan cara yang menghabiskan banyak waktu serta biaya yang besar.

Sebaliknya *white-box* merupakan jenis pengujian yang berbalikan dengan *black-box* karena semua informasi secara lengkap diberitahukan di depan serta infrastruktur mana saja yang perlu diuji, pengujian ini mirip dengan tindakan sebagai karyawan perusahaan. Cara pengujian ini dibagi menjadi 2 bagian yakni yang diberitahukan dengan kerjasama sepenuhnya oleh karyawan IT maupun yang tidak diberitahukan dimana tanpa sepengetahuan staff IT.

Jenis yang terakhir adalah *grey-box* dimana campuran keduanya melibatkan informasi yang terbatas serta pengujian secara internal, selain itu setiap program diteliti untuk celahnya. Simulasi yang digunakan di *grey-box* berdasarkan pengujian *black-box* serta pengetahuan yang ada untuk mendapatkan analisa secara menyeluruh.

3.4 Alur Pengujian Penelitian



Gambar 1 *Flowchart* Alur Pengujian Penelitian

Berdasarkan ilustrasi pada Gambar 1, dalam langkah awal pengujian penelitian perlu dilakukan pengumpulan informasi mengenai posisi fisik *server*, jenis jaringan yang digunakan, perangkat yang digunakan dan berbagai informasi yang berkaitan dengan *server* Universitas Kristen Petra yang bisa didapatkan dengan aplikasi ID Serve, HTTPRecon, situs Who.Is, NSLookup dan NetCraft, kemudian dilakukan pemindaian celah yang ada pada sistem dengan menggunakan aplikasi *Acunetix* dan OpenVAS. Setelah selesai, pemindaian kata sandi juga dilakukan guna mencari titik lemah kata sandi yang digunakan dalam sistem dengan aplikasi THC-Hydra. Selain dari segi perangkat lunak yang berjalan, akses fisik juga perlu diuji baik dari siapa saja yang berhak mengakses ruangan *server*, peletakan *server* maupun penataan kabel jaringan dari ruang *server*, serta hal – hal yang berkaitan dengan akses fisik lainnya berdasarkan skema ISO 27001. Setelah semua selesai diuji maka laporan akan dibuat dengan standar dari *template* pengujian yang disediakan oleh EC-Council dalam modul LPT sebagai standar yang digunakan secara umum oleh para ahli *security analyst*.

Berdasarkan teori yang dijelaskan pada subbab sebelumnya, penelitian ini akan dijalankan dengan metode *grey-box* dan diposisikan sebagai tim biru karena skema infrastruktur yang ada di Universitas Kristen Petra sudah diberikan sebelumnya dan dibutuhkan pemindaian yang sudah diketahui oleh pihak yayasan. Selain itu sifat pengujian ini sebatas non-destruktif dikarenakan jika dilakukan kegiatan pengujian seperti *Denial of Service* dapat mengakibatkan gangguan pada kegiatan administrasi.

4. IMPLEMENTASI APLIKASI

Dalam bab ini, akan dijelaskan secara singkat *tools* atau alat yang digunakan dalam pengujian penelitian ini. Alat – ini terambil dari standar yang digunakan dalam modul CEH.

4.1 WHOIS

Bersumber dari situs Internet Corporation for Assigned Names and Numbers (ICANN), WHOIS adalah protokol *query* dan respon yang banyak digunakan untuk men-*query database* yang menyimpan pengguna terdaftar ataupun sumber daya internet seperti nama *domain*, blok alamat IP, atau sistem otomasi, tapi juga digunakan untuk berbagai kebutuhan informasi lainnya. Protokol ini menyimpan dan mengirimkan isi *database* dalam format yang bisa dibaca manusia.

4.2 NSLookup

Bersumber dari manual yang tersimpan dalam sistem operasi UNIX, *Nslookup* adalah alat *command-line* untuk administrasi jaringan yang tersedia di semua sistem operasi komputer untuk mendapatkan informasi *record Domain Name System*. Dalam pengembangan BIND 9, Konsortium Sistem Internet ingin menggantikan nslookup menjadi *host* dan *dig*. Namun keputusan ini dibatalkan pada tahun 2004 saat peluncuran BIND 9.3 dan akhirnya ada dukungan penuh untuk fungsi *nslookup*.

NSLookup berarti *Name Server Lookup*. *Nslookup* tidak menggunakan *library* DNS untuk melakukan *query* sehingga beberapa hasilnya terkadang berbeda dengan fungsi *dig*.

Nslookup bisa dioperasikan dengan mode interaktif dan non interaktif. Ketika modenya interaktif, bisa digunakan dengan argumen seperti program pada umumnya. Jika dioperasikan pada mode non interaktif, informasi yang dicari hanya berdasarkan argumen yang dipersiapkan sebelumnya sesuai dengan *webserver* yang akan dituju.

4.3 NetCraft

Netcraft adalah perusahaan layanan internet di Inggris. *Netcraft* dibiayai dengan menyediakan layanan seperti: menyediakan layanan keamanan internet, termasuk pengujian aplikasi, ulas balik kode, dan otomasi ujicoba penetrasi. Selain itu menyediakan data dan analisa dari segala aspek internet.

4.4 ID Serve

Berdasarkan situs GRC.com, ID Serve merupakan *freeware* yang dikembangkan oleh Steve Gibson yang berguna untuk alat investigasi keamanan esensial. Fungsi utamanya adalah untuk memeriksa sebuah kinerja *webserver*. Program ini mampu

memberikan informasi mengenai sistem operasi yang digunakan di *server*. Selain itu fungsi tambahan yang memberikan informasi seperti *cookie* dan *reverse DNS* juga tersedia. *Gibson Research Corp.* telah mengembangkan berbagai perangkat lunak yang berguna bagi konsumen. Biasanya alat yang dikembangkan meliputi :

- Menemukan celah yang ada di *server*
- Konfigurasi filter *firewall*
- Identifikasi *server* HTTP dan non HTTP
- Pencarian *reverse* DNS dengan menggunakan DNS untuk menemukan alamat IP

ID Serve sangat berguna dalam membuat sebuah pengujian terhadap keamanan sebuah *webserver*. ID Serve berfungsi untuk memberikan *cookies* sebuah situs dan mampu memperlihatkan kepada pengguna dari segi format, penampilan dan informasi sejenisnya. Selain itu aplikasi ini dapat memberikan status sebuah *port* apakah ditutup atau tersembunyi. Fungsi utama ID *Serve* adalah melacak sebuah nama *domain* yang merujuk pada sebuah alamat IP yang muncul di *log firewall* komputer pengguna. Selain itu aplikasi ini dapat meyakinkan pengguna situs komersial keamanan yang lebih pasti.

4.5 HTTPRecon

Berdasarkan situs yang dibuat oleh Marc Ruef sebagai perancang perangkat lunak Httprecon, Httprecon didefinisikan sebagai alat untuk *fingerprinting* sebuah situs. Proyek ini bergerak di bidang riset *fingerprinting* HTTP. Tujuannya adalah mengidentifikasi implementasi HTTPD secara lengkap yang dapat membantu analisa potensi celah. Selain itu cara pendekatannya dilakukan dari berbagai sumber yang terotomasi juga disediakan dalam aplikasi dan diharapkan aplikasi ini mempermudah dan meningkatkan efisiensi dalam enumerasi seperti ini. Cara pendekatan seperti *banner-grabbing*, enumerasi kode status dan analisa urutan *header* juga digunakan. Dengan banyak teknik analisa yang juga diperkenalkan maka dapat membantu keakuratan *fingerprinting* sebuah *webserver*.

4.6 OpenVAS

Berdasarkan situs OpenVAS.org, *OpenVAS* (*Open Vulnerability Assessment System*) merupakan sebuah *framework* yang terdiri atas beberapa layanan dan alat yang menawarkan untuk pencarian celah keamanan dan memberikan solusinya. Program ini tersedia secara cuma – cuma dan hampir semua komponen dilisensi dibawah GPL, versi yang terbaru adalah 8.0. Dalam penelitian ini, OpenVAS berjalan dalam sebuah *Virtual Machine Oracle VirtualBox*, sehingga untuk menjalankan fitur diperlukan peramban.

5. PENGUJIAN APLIKASI

5.1 Information Gathering

5.1.1 WHOIS

Dengan bantuan situs seperti *DomainTools*, informasi mengenai sejarah sebuah *domain* tercantum dan dilampirkan dalam format WhoIs, dimana informasi seperti tanggal pembuatan *domain*, nama pemilik *domain* dan informasi sederhana seperti jenis *server* yang digunakan, lokasi dan alamat IP terlampir di dalamnya. Pemilik *domain* www.petra.ac.id beserta *subdomain*-nya tercantum atas nama Bapak Justinus Andjarwirawan.

5.1.2 NSLookup

Domain www.petra.ac.id termasuk dalam *domain* PANDI. D*omain* petra.ac.id memiliki alamat IP 203.189.120.27, dengan *Mail Exchanger* milik *Google* serta *Nameserver* yang berada di *server* lokal milik petra dengan nama *Peter* dan *Jacob* kemudian *backup* DNS di *ZoneEdit*. Ada pula DNS tipe TXT yang mencantumkan alamat asal www.petra.ac.id agar ketika mengirim *e-mail*, *hosting* penerima tidak menolak karena keberadaannya sudah diakui. *Domain* lain seperti dewey.petra.ac.id serta bakp.petra.ac.id hanya menampilkan *canonical name* atau alias lain yang digunakan untuk *subdomain* mereka yakni digilib.petra.ac.id untuk *Dewey* dan cpanely.petra.ac.id untuk bakp.petra.ac.id. sedangkan untuk situs sim.petra.ac.id hasil yang didapatkan adalah alamat IP 203.189.120.131.

5.2 Webserver Footprinting

5.2.1 NetCraft

Situs www.petra.ac.id pertama kali terlihat di dunia maya pada bulan Mei 1996. Situs ini dimiliki oleh Universitas Kristen Petra dan sudah terjadi beberapa kali perpindahan *hosting* dari PT Telkom Indonesia kemudian dikembangkan dan dirawat oleh yayasan Universitas Kristen Petra, hal ini terlihat dari pergantian *Netblock owner* yang mengidentifikasi mengenai kepemilikan suatu alamat IP. Selain itu ada 3 kali lagi pergantian *hosting* dari alamat 203.130.237.183 ke 203.189.120.179 dan berganti lagi hingga saat ini menjadi 203.189.120.27.

Situs sim.petra.ac.id pertama kali muncul pada bulan Agustus 2011 dengan alamat IP 203.189.120.131. Tidak ada sejarah pergantian *server* pada situs ini namun terlihat ada tindakan *reboot* 40 hari yang lalu.

Situs dewey.petra.ac.id pertama kali muncul pada bulan November 2001 yang bersifat katalog *online* perpustakaan. Situs ini juga berada di bawah kepemilikan yayasan dan telah berpindah *hosting* sebanyak 3 kali dari 202.43.253.210 ke 203.189.120.206 menjadi 203.189.120.205.

Sedangkan situs terakhir yakni bakp.petra.ac.id pertama kali muncul pada bulan Juni 2012 dan tidak ada sejarah perpindahan *server* maupun aktivitas *reboot* belum pernah terlihat karena situs ini belum pernah tercantum dalam *database NetCraft*. Alamat IP situs ini adalah 203.189.120.28.

5.2.2 ID Serve

Aplikasi berikut ini memeriksa jenis *server* yang digunakan dari *header* yang tercantum saat meminta *request* pada situs tersebut.

Dari hasil pengujian situs www.petra.ac.id dapat diidentifikasi *server* yang digunakan adalah Apache versi 2.2.21 di sistem operasi Unix dan menggunakan SSL OpenSSL versi 0.9.8. Sementara sim.petra.ac.id teridentifikasi sebagai Apache versi 2.2.9 dengan sistem operasi Debian dan berjalan dengan PHP versi 5.2.6.1.

Selanjutnya situs bakp.petra.ac.id berjalan pada sistem operasi Unix dengan menggunakan Apache versi 2.2.27 sebagai *webserver* dan juga menggunakan modul SSL OpenSSL versi 0.9.8. Yang terakhir adalah situs dewey.petra.ac.id, situs ini berjalan pada sistem operasi Debian dengan *webserver* Apache versi 2.2.16.

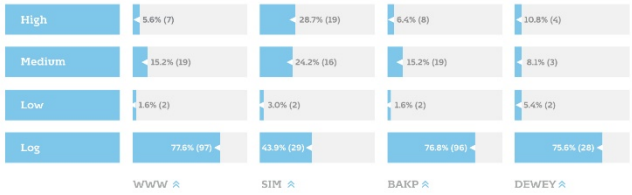
5.2.3 HTTPRecon

Berdasarkan hasil pengujian, www.petra.ac.id memiliki versi *webserver* httpd Apache 1.3.33. Sementara untuk situs dewey.petra.ac.id menggunakan Apache 2.0.55. Hasil pengujian sim.petra.ac.id menunjukkan Apache 2.0.55 juga digunakan di situs ini. Yang terakhir situs bakp.petra.ac.id menggunakan Apache versi 2.0.52 pada situs ini.

5.3 Vulnerability Scanning

5.3.1 OpenVAS

Berdasarkan Gambar 2, hasil analisa dari situs dewey.petra.ac.id memiliki 4 celah dengan tingkat *high*, 3 celah dengan tingkat *medium*, 2 celah dengan tingkat *low*, dan 28 celah dengan tingkat *log*. Sedangkan untuk www.petra.ac.id memiliki 7 celah dengan tingkat *high*, 19 celah dengan tingkat *medium*, 2 celah dengan tingkat *low*, dan 97 celah dengan tingkat *log*. Situs bakp.petra.ac.id memiliki 8 celah kemanan tingkat *high*, 19 celah dengan tingkat *medium*, 2 celah dengan tingkat *low*, dan 96 celah dengan tingkat *log*. Yang terakhir situs sim.petra.ac.id memiliki jumlah celah terbanyak yaitu 19 celah dengan tingkat *high*, 16 celah dengan tingkat *medium*, dan 2 celah tingkat *low*, dan 29 celah dengan tingkat *log*.



Gambar 2 Grafik Jumlah Celah Berdasarkan Hasil Pemindaian Celah dengan Perangkat Lunak OpenVAS

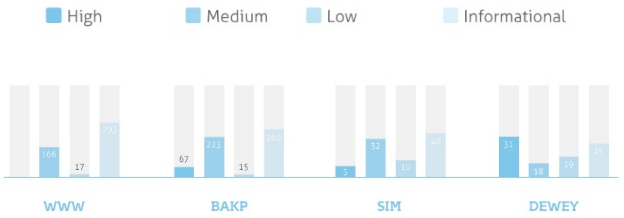
Vulnerabilities	www.petra.ac.id	sim.petra.ac.id	bakp.petra.ac.id	dewey.petra.ac.id
OpenSSL	✓	✓	✓	✓
Apache outdated		✓		
HTTP Test Method	✓		✓	
XSS	✓		✓	
Wordpress	✓		✓	
Apache file listing	✓		✓	
openssh	✓	✓		✓

Gambar 3 Tabel Rangkuman Pemindaian Celah dengan Perangkat Lunak OpenVAS

Berdasarkan rangkuman celah keamanan yang sudah digolongkan terlampir pada gambar 3 di atas, meski Sim.petra.ac.id memiliki banyak masalah kerentanan tetapi memiliki sifat celah keamanan yang sama sehingga seperti masalah OpenSSL dan Apache bisa diselesaikan dengan memperbarui dengan pembaruan yang tersedia. Lain dengan situs Www.petra.ac.id dan Bakp.petra.ac.id yang memiliki variasi celah yang memungkinkan dapat diserang karena varian celah yang ada pada situs tersebut lebih banyak.

5.3.2 Acunetix

Berdasarkan Gambar 4, hasil pemindaian celah dari situs www.petra.ac.id dengan jumlah peringatan 476 buah yang terdiri atas 0 peringatan tingkat tinggi, 166 peringatan tingkat sedang, 17 peringatan tingkat rendah dan 293 peringatan informasi. Sementara untuk situs bakp.petra.ac.id memiliki jumlah peringatan sebanyak 565 peringatan dengan rincian 67 peringatan tingkat tinggi, 223 peringatan tingkat sedang, 15 peringatan tingkat rendah dan 260 peringatan informasi. Untuk situs dewey.petra.ac.id memiliki jumlah peringatan lebih sedikit yaitu 93 peringatan yang terdiri atas 31 peringatan tingkat tinggi, 18 peringatan tingkat sedang, 19 peringatan tingkat rendah, 25 peringatan informasi. Situs yang terakhir sim.petra.ac.id memiliki jumlah peringatan paling rendah yaitu sebanyak 87 peringatan, terdiri dari 5 peringatan tingkat tinggi, 32 peringatan tingkat sedang, 10 peringatan tingkat rendah, dan 40 peringatan informasi.



Gambar 4 Grafik Jumlah Celah Berdasarkan Hasil Pemindaian Celah dengan Perangkat Lunak Acunetix WVS

Vulnerabilities	www.petra.ac.id	sim.petra.ac.id	bakp.petra.ac.id	dewey.petra.ac.id
SQL Injection		✓		✓
XSS			✓	✓
DoS	✓	✓	✓	✓
Clickjacking	✓	✓	✓	✓
Cookie	✓	✓	✓	✓
Directory/file listing	✓	✓	✓	✓
Slow response	✓	✓	✓	✓

Gambar 5 Tabel Rangkuman Pemindaian Celah dengan Perangkat Lunak Acunetix WVS

Berdasarkan hasil pemindaian di Gambar 5, celah yang dimiliki oleh setiap situs identik yang menandakan bahwa setiap situs dapat diserang dengan metode yang sama. Selain itu serangan umum seperti DoS dapat dilakukan pada semua situs yang diuji pada penelitian ini. Beberapa perbaikan dari penggolongan celah di atas memerlukan perubahan konfigurasi *server*.

5.4 Analisa

5.4.1 Perbandingan Hasil Pemindaian Antara OpenVAS dan Acunetix Web Vulnerability Scanner

Pada dasarnya analisa yang diberikan memiliki kecenderungan yang berbeda dimana OpenVAS lebih menganalisa sistem dari sisi akses luar menuju sistem sehingga kurang terperinci bagian dari situs mana saja yang terpengaruh. Sementara Acunetix WVS lebih memperinci bagian situs mana saja yang perlu ditelusuri lebih lanjut. Dari cara penyajian laporan Acunetix memiliki kemampuan lebih jauh yang bisa diberikan pada manajer maupun para *programmer* untuk dapat mengerti permasalahan yang dihadapi pada suatu aplikasi situs yang dibuat.

Perangkat lunak Acunetix memindai lebih lengkap dari segi performa situs beserta keamanannya, namun dari sisi keamanan *server* cukup kurang pemindaiannya. Sebaliknya OpenVAS cenderung memeriksa keamanan situs namun tidak terlalu memperhatikan performa situs.

Keakuratan kedua perangkat lunak ini tidak menjamin bahwa analisanya tepat karena masih tetap ada ketergantungan dengan informasi yang didapatkan dari *banner*.

Kedua perangkat lunak menunjukkan seberapa rentan sebuah situs terhadap celah yang disediakan dalam pengujian, namun untuk memastikan bahwa celah tersebut ada, dibutuhkan akses yang tidak didapatkan pada riset ini karena konfidensial isi sistem terhadap penguji.

5.4.2 Perbandingan Hasil Pemindaian Antara OpenVAS dan Acunetix Web Vulnerability Scanner

HTTPRecon dan ID Serve seringkali memberikan hasil yang berbeda dan diperlukan penentuan *tools* mana yang lebih baik. Jika dibandingkan dengan cara pengujian, ID Serve hanya

menggunakan informasi *banner* sedangkan HTTPRecon menggunakan metode *fingerprint* dan membandingkan dengan database untuk menemukan versi *server* yang digunakan.

Metode *banner-grabbing* secara umum sering digunakan, namun dengan adanya server hardening, server tidak mudah untuk langsung diidentifikasi karena konfigurasi *banner*nya sudah berubah untuk mengurangi kemungkinan bisa ditemukan celah untuk penyerangan.

5.4.3 Halangan Atau Kendala Selama Pengujian Penetration Testing

Terdapat beberapa halangan yang ada dalam pengujian yakni ketersediaan *resource* jika dilakukan uji coba secara mendalam karena waktu pemindaian 1 situs tidaklah pendek, jika menggunakan konfigurasi bawaan, untuk membuat kombinasi suatu situs diperlukan waktu lebih dari 3 hari dan waktu pemindaiannya lebih dari 3 minggu dimana jika dilakukan secara terus menerus maka ISP Petra akan beresiko terblokir karena layanan ini cukup intensif dalam menggunakan *request* menuju situs.

Selain itu terjadi permasalahan yakni karena ketidakamanan situs Universitas Kristen Petra, terjadi kasus *spamming* pada *email* dosen dan organisasi di dalam Universitas Kristen Petra ketika pengujian karena tidak ada *captcha code* pada form pengunduran diri dan cuti studi, namun setelah kejadian ini. *Programmer* Universitas Kristen Petra telah memperbaiki masalah ini.

Dan untuk mencegah terjadi kejadian yang tidak diharapkan maka pengujian seperti pembobolan kata sandi, pengujian DoS, dan pengujian lainnya dihentikan.

5.4.4 Hasil Pengujian Keamanan Secara Keseluruhan

Keamanan sistem baik situs maupun administrasi yang diuji dalam penelitian ini secara garis besar tergolong buruk, karena kurang perawatan pada sistem seperti pembaruan berkala, sehingga terjadi beberapa kasus yang seharusnya tidak terjadi tetapi berakibat fatal ketika diserang. Untuk situs sim.petra.ac.id masih tergolong baik karena celah dengan tingkat tinggi sudah cukup sedikit namun dengan memastikan bahwa sistem diperbarui dengan baik maka celah bisa dikurangi hingga sesedikit mungkin. Namun lain halnya untuk situs lainnya, mereka terkena efek SQL *Injection* karena kurangnya pengamanan pada fitur metakarakter yang seharusnya bisa dengan mudah disaring untuk menghindari SQL *Injection*. Selain itu juga terdapat masalah pada sistem karena tidak semua berjalan pada *platform* yang sama dan memiliki versi Apache yang bervariatif.

Berdasarkan hasil pemindaian celah, ditemukan bahwa celah terbanyak pada tingkat sedang baik dari hasil pemindaian OpenVAS maupun Acunetix. Celah yang banyak ditemukan berasal dari celah yang bergantung pada SSL dan *Cross Site Scripting*. Selain itu dominasi *Denial of Service* cukup berperan banyak pada keempat situs yang diuji yang artinya situs rentan untuk dilakukan *overloading* sehingga situs tidak dapat melayani pengguna.

Selain permasalahan yang disebutkan, direktori sering dapat diakses secara langsung yang beresiko untuk terbongkar sehingga situs dapat dijelajahi dan ada kemungkinan *file* dapat diunduh oleh penyerang untuk dilakukan information gathering dan kemudian dianalisa untuk dijadikan strategi penyerangan. Selain itu potensi performa situs yang lambat juga rentan membawa koneksi situs untuk di-*flooding* untuk *denial of service*.

6. DAFTAR REFERENSI

[1] Red Hat, Inc. 42.1.1. What is Computer Security? *42.1.1. What is Computer Security?* [Online] 07 26, 2007. [Cited: 10 22, 2014.] https://www.centos.org/docs/5/html/5.1/Deployment_Guide/s1-sgs-ov-cs.html.

[2] Ruef, Marc. httprecon project / faq. *httprecon project.* [Online] 2015. http://www.computec.ch/projekte/httprecon/?s=faq.

[3] Hariwibowo, Dody. Keamanan Komputer | Pengantar Teknologi Informasi. *Pengantar Teknologi Informasi.* [Online] 02 06, 2011. [Cited: 10 21, 2014.] http://dhoddycreater.wordpress.com/makalah-pti/keamanan-komputer.

[4] Gibson, Steve. GRC | ID Serve - Internet Server Identification Utility. *GRC | ID Serve - Internet Server Identification Utility.* [Online] Oct 06, 2003. https://www.grc.com/id/idserve.htm.

[5] Barnatt, Christopher. ExplainingComputer.com: Computer Security. *ExplainingComputer.com.* [Online] 09 13, 2012. [Cited: 10 20, 2014.] http://explainingcomputer.com/security.html.

[6] Acunetix. Web Application Security with Acunetix Web Vulnerability Scanner. *Web application security with Acunetix.* [Online] 2015. https://www.acunetix.com/vulnerability-scanner/.

[7] OpenVAS. OpenVAS - About OpenVAS Software. *OpenVAS - OpenVAS - Open Vulnerability Assessment System.* [Online] 2015. http://www.openvas.org/software.html.

[8] EC-Council. *Certified Ethical Hacker v8 : Module 20 Penetration Testing.* Amerika : EC-Council, 2012.

[9] —. *Certified Ethical Hacker v8 : Module 12 Hacking Webservers.* Amerika : EC-Council, 2012.

[10] PortSwigger Ltd. Burp Suite. *Burp Suite.* [Online] http://portswigger.net/burp/.

[11] Tenable Network Security ®. Nessus Vulnerability Scanner | Tenable Network Security. *Tenable Network Security.* [Online] http://www.tenable.com/products/nessus-vulnerability-scanner.

[12] Peck, Dave. Cloak's super-simple VPN blog. *Cloak's super-simple VPN blog: Let's hack things with Firesheep.* [Online] 07 15, 2013. https://blog.getcloak.com/2013/07/15/lets-hack-things-firesheep/.

[13] Internet Corporation for Assigned Names and Numbers. WHOIS Primer | ICANN WHOIS. *ICANN WHOIS.* [Online] http://whois.icann.org/en/primer.

[14] Computer Hope. Linux and Unix nslookup command help and examples. *Linux and Unix nslookup command help and examples.* [Online] http://www.computerhope.com/unix/unslooku.htm.

[15] EC-Council. *Certified Ethical Hacker v8 : Modul 10 Sniffing, Spoofing, Hijacking.* Amerika : EC-Council, 2012.

[16] —. *EC-Council Certified Security Analyst 4.0 Official Course LPT Chapter XXIX Physical Security Penetration Testing.* Amerika : s.n., 2013.